



## PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10020780 A**(43) Date of publication of application: **23.01.98**

(51) Int. Cl. **G09C 1/00**  
**G09C 1/00**  
**H04L 9/32**

(21) Application number: **08168965**(71) Applicant: **SONY CORP**(22) Date of filing: **28.06.96**

(72) Inventor: **KUSAKABE SUSUMU**  
**TAKADA MASAYUKI**

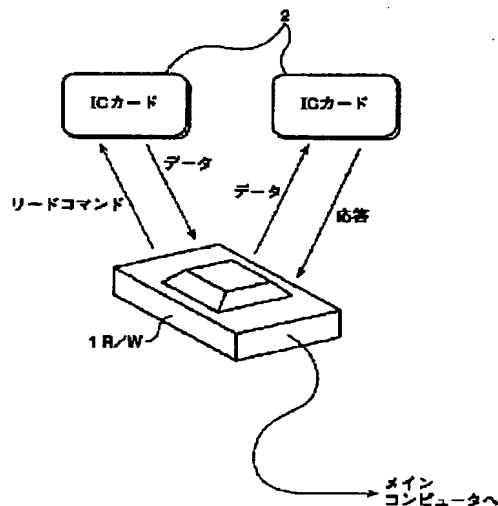
(54) **CERTIFICATION METHOD, COMMUNICATION  
METHOD AND INFORMATION PROCESSING  
DEVICE**

## (57) Abstract:

**PROBLEM TO BE SOLVED:** To perform the certification mutually, by enciphering a clear text mutually received, to transmit the same to a device which has transmitted the clear text, and comparing the clear text obtained by decoding the received cipher text, with the clear text which has been transmitted first.

**SOLUTION:** A reader writer(R/W) 1 enciphers random numbers RA to a cipher  $C_1$  with a key KLB, and an IC card 2 encodes the cipher  $C_1$  to a clear text  $M_1$  with the key KB. The IC card 2 enciphers the clear text  $M_1$  to a cipher  $C_2$  with a key KA, the random number RB is enciphered to a cipher  $C_3$  with the key KA, and R/W 1 encodes the cipher  $C_2$  to the clear text  $M_2$  with the key KA. And the R/W 1 certifies the IC card 2 when the clear text  $M_2$  and the random number RA are judged to be same as each other. In the next, R/W 1 encodes the cipher  $C_3$  to a clear text  $M_3$  with the key KA, the clear text  $M_3$  is encoded to a cipher  $C_4$  with the key KB, and the IC card 2 encodes the cipher  $C_4$  to the clear text  $M_4$  with the key KB. And the IC card 2 certifies R/W1, when the clear text  $M_4$  and the random number RB are judged to be same as each other.

COPYRIGHT: (C)1998,JPO



(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開平10-20780

(43)公開日 平成10年(1998)1月23日

(51)Int.Cl. <sup>8</sup>	識別記号	庁内整理番号	FI	技術表示箇所
G 0 9 C 1/00	6 4 0	7259-5J	G 0 9 C 1/00	6 4 0 A
		7259-5J		6 4 0 E
	6 6 0	7259-5J		6 6 0 A
H 0 4 L 9/32			H 0 4 L 9/00	6 7 5 A

審査請求 未請求 請求項の数30 OL (全 18 頁)

(21)出願番号 特願平8-168965

(22)出願日 平成8年(1996)6月28日

(71)出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72)発明者 日下部 進

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72)発明者 高田 昌幸

東京都品川区北品川6丁目7番35号 ソニー株式会社内

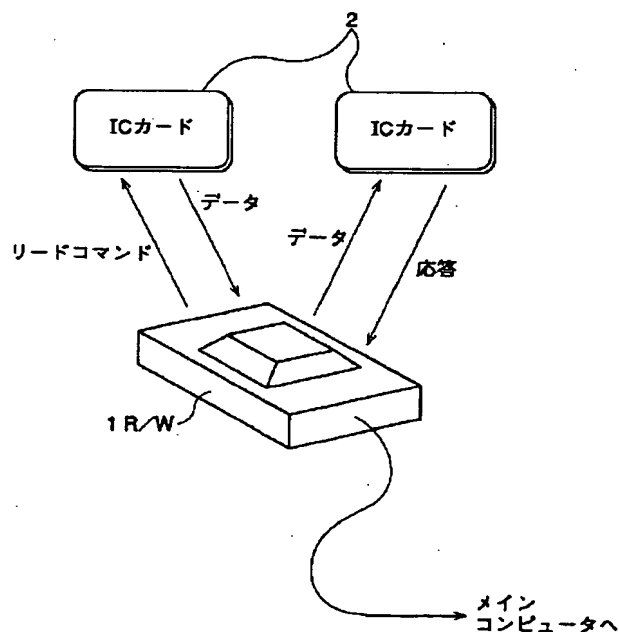
(74)代理人 弁理士 稲本 義雄

(54)【発明の名称】 認証方法、通信方法、および、情報処理装置

(57)【要約】

【課題】 相互に認証を行う。

【解決手段】 R/W1は、乱数R<sub>A</sub>を鍵K<sub>A</sub>で暗号化した暗号C<sub>1</sub>をICカード2に送信する。ICカード2は、その暗号C<sub>1</sub>を鍵K<sub>A</sub>で平文M<sub>1</sub>に復号化する。ICカード2は、平文M<sub>1</sub>を鍵K<sub>A</sub>で暗号化した暗号C<sub>2</sub>と、乱数R<sub>B</sub>を鍵K<sub>A</sub>で暗号化した暗号C<sub>3</sub>をR/W1に送信する。R/W1は、その暗号C<sub>2</sub>、C<sub>3</sub>を、鍵K<sub>A</sub>で平文M<sub>2</sub>と平文M<sub>3</sub>にそれぞれ復号化する。R/W1は、平文M<sub>2</sub>と乱数R<sub>A</sub>が同一であると判断した場合、ICカード2を認証する。次に、R/W1は、平文M<sub>3</sub>を鍵K<sub>A</sub>で暗号化した暗号C<sub>4</sub>をICカード2に送信する。ICカード2は、その暗号C<sub>4</sub>を、鍵K<sub>A</sub>で平文M<sub>4</sub>に復号化する。ICカード2は、平文M<sub>4</sub>と乱数R<sub>B</sub>が同一であると判断した場合、R/W1を認証する。



## 【特許請求の範囲】

【請求項1】 第1の鍵および第2の鍵を記憶する記憶手段と、

所定のデータを前記第1の鍵または前記第2の鍵を利用して暗号化する暗号化手段と、

前記第2の鍵または前記第1の鍵による暗号を復号化する復号化手段とをそれぞれ備える第1の情報処理装置と第2の情報処理装置との間における認証方法において、前記第1の情報処理装置の前記暗号化手段が、前記第1の鍵で、第1のデータを第1の暗号に暗号化するステップと、

前記第2の情報処理装置の前記復号化手段が、前記第1の鍵で、前記第1の暗号を第2のデータに復号化するステップと、

前記第2の情報処理装置の前記暗号化手段が、前記第2の鍵で、前記第2のデータを第2の暗号に暗号化するステップと、

前記第2の情報処理装置の前記暗号化手段が、前記第2の鍵で、第3のデータを第3の暗号に暗号化するステップと、

前記第1の情報処理装置の前記復号化手段が、前記第2の鍵で、前記第2の暗号を第4のデータに復号化するステップと、

前記第1の情報処理装置が、前記第1のデータと前記第4のデータに応じて、前記第2の情報処理装置を認証するステップと、

前記第1の情報処理装置の前記復号化手段が、前記第2の鍵で、前記第3の暗号を第5のデータに復号化するステップと、

前記第1の情報処理装置の前記暗号化手段が、前記第1の鍵で、前記第5のデータを第4の暗号に暗号化するステップと、

前記第2の情報処理装置の前記復号化手段が、前記第1の鍵で、前記第4の暗号を第6のデータに復号化するステップと、

前記第2の情報処理装置が、前記第3のデータと前記第6のデータに応じて、前記第1の情報処理装置を認証するステップとを備えることを特徴とする認証方法。

【請求項2】 第1の鍵および第2の鍵を記憶する記憶手段と、

所定のデータを前記第1の鍵または前記第2の鍵を利用して暗号化する暗号化手段と、

前記第2の鍵または前記第1の鍵による暗号を復号化する復号化手段と、

暗号化された前記データを送信する送信手段と、

所定の暗号化されたデータを受信する受信手段とを備える第1の情報処理装置と第2の情報処理装置との間における通信方法において、

前記第1の情報処理装置の前記暗号化手段が、前記第1の鍵で、第1のデータを第1の暗号に暗号化するステッ

プと、

前記第1の情報処理装置の前記送信手段が、前記第1の暗号を、前記第2の情報処理装置に送信するステップと、

前記第2の情報処理装置の前記受信手段が、前記第1の暗号を受信するステップと、

前記第2の情報処理装置の前記復号化手段が、前記第1の鍵で、前記第1の暗号を第2のデータに復号化するステップと、

10 前記第2の情報処理装置の前記暗号化手段が、前記第2の鍵で、前記第2のデータを第2の暗号に暗号化するステップと、

前記第2の情報処理装置の前記暗号化手段が、前記第2の鍵で、第3のデータを第3の暗号に暗号化するステップと、

前記第2の情報処理装置の前記送信手段が、前記第2の暗号および前記第3の暗号を、前記第1の情報処理装置に送信するステップと、

20 前記第1の情報処理装置の前記受信手段が、前記第2の暗号および前記第3の暗号を受信するステップと、

前記第1の情報処理装置の前記復号化手段が、前記第2の鍵で、前記第2の暗号を第4のデータに復号化するステップと、

前記第1の情報処理装置が、前記第1のデータと前記第4のデータに応じて、前記第2の情報処理装置を認証するステップと、

前記第1の情報処理装置の前記復号化手段が、前記第2の鍵で、前記第3の暗号を第5のデータに復号化するステップと、

30 前記第1の情報処理装置の前記暗号化手段が、前記第1の鍵で、前記第5のデータを第4の暗号に暗号化するステップと、

前記第1の情報処理装置の前記送信手段が、前記第4の暗号を、前記第2の情報処理装置に送信するステップと、

前記第2の情報処理装置の前記受信手段が、前記第4の暗号を受信するステップと、

前記第2の情報処理装置の前記復号化手段が、前記第1の鍵で、前記第4の暗号を第6のデータに復号化するステップと、

40 前記第2の情報処理装置が、前記第3のデータと前記第6のデータに応じて、前記第1の情報処理装置を認証するステップとを備えることを特徴とする通信方法。

【請求項3】 前記第1のデータは、所定の認識番号であり、

前記第3のデータは、第3の鍵であり、

前記第1の情報処理装置の前記暗号化手段は、第1のコマンドを、前記第3の鍵で第5の暗号に暗号化するとともに、前記認識番号を、前記第3の鍵で第6の暗号に暗号化し、

50

前記第1の情報処理装置の前記送信手段は、前記第5の暗号を、前記第6の暗号とともに送信し、  
 前記第2の情報処理装置の前記受信手段は、前記第5の暗号および前記第6の暗号を受信し、  
 前記第2の情報処理装置の前記復号化手段は、前記第5の暗号を、前記第3の鍵で第2のコマンドに復号化するとともに、前記第6の暗号を、前記第3の鍵で第7のデータに復号化し、  
 前記第2の情報処理装置は、前記第7のデータと前記認識番号の値に応じて、前記第2のコマンドを承認すること

を特徴とする請求項2に記載の通信方法。  
 【請求項4】 前記第1の情報処理装置の前記認識番号は、前記第1のコマンドの暗号化毎に変更されることを特徴とする請求項3に記載の通信方法。

【請求項5】 前記第1の情報処理装置の前記認識番号は、前記第1のコマンドの暗号化毎に増加されることを特徴とする請求項4に記載の通信方法。

【請求項6】 前記第2の情報処理装置は、前記第7のデータが前記認識番号に対応する所定の範囲内の値であるとき、前記第2のコマンドを承認すること

を特徴とする請求項3に記載の通信方法。  
 【請求項7】 前記第2の情報処理装置は、前記第7のデータと前記認識番号の値を所定の桁数の範囲だけにおいて比較し、前記第7のデータにおける前記所定の桁数の範囲の値が、前記認識番号における前記所定の桁数の範囲の値以上であるとき、前記第2のコマンドを承認すること

を特徴とする請求項3に記載の通信方法。  
 【請求項8】 前記第2の情報処理装置は、前記第2のコマンドに対応する処理を行い、その処理の結果に対応する応答データを生成し、

前記第2の情報処理装置の前記暗号化手段は、前記応答データを、前記第3の鍵で第7の暗号に暗号化するとともに、前記認識番号を、前記第3の鍵で第8の暗号に暗号化し、

前記第2の情報処理装置の前記送信手段は、前記第7の暗号を、前記第8の暗号とともに送信し、

前記第1の情報処理装置の前記受信手段は、前記第7の暗号および前記第8の暗号を受信し、

前記第1の情報処理装置の前記復号化手段は、前記第7の暗号を、前記第3の鍵で第8のデータに復号化するとともに、前記第8の暗号を、前記第3の鍵で第9のデータに復号化し、

前記第1の情報処理装置は、前記第9のデータと前記認識番号の値に応じて、前記第8のデータを、前記応答データとして承認すること

を特徴とする請求項3に記載の通信方法。  
 【請求項9】 前記第2の情報処理装置の前記認識番号は、前記第8のデータの暗号化毎に変更されることを特徴とする請求項8に記載の通信方法。

【請求項10】 前記第2の情報処理装置の前記認識番

号は、前記第8のデータの暗号化毎に増加されることを特徴とする請求項9に記載の通信方法。

【請求項11】 前記第1の情報処理装置は、前記第9のデータが前記認識番号に対応する所定の範囲内の値であるとき、前記第8のデータを、前記応答データとして承認すること

を特徴とする請求項8に記載の通信方法。  
 【請求項12】 前記第1の情報処理装置は、前記第9のデータと前記認識番号の値を所定の桁数の範囲だけにおいて比較し、前記第9のデータにおける前記所定の桁数の範囲の値が、前記認識番号における前記所定の桁数の範囲の値以上であるとき、前記第8のデータを、前記応答データとして承認すること

を特徴とする請求項8に記載の通信方法。  
 【請求項13】 前記第1の情報処理装置は、前記第5の暗号を、前記第6の暗号とともに送信した後、前記7の暗号および前記第8の暗号を受信するまでに所定の時間が経過した場合、前記認識番号の値を増加した後、前記認識番号を前記第6の暗号に暗号化し、前記第5の暗号を、前記第6の暗号とともに再送すること

を特徴とする請求項8に記載の通信方法。  
 【請求項14】 前記第1の情報処理装置は、前記第8のデータを、応答データとして承認しない場合、前記認識番号の値を増加した後、前記認識番号を前記第6の暗号に暗号化し、前記第5の暗号を、前記第6の暗号とともに再送すること

を特徴とする請求項8に記載の通信方法。  
 【請求項15】 第1の鍵および第2の鍵を記憶する記憶手段と、

所定のデータを、前記第1の鍵または前記第2の鍵を利用して暗号化する暗号化手段と、

前記第2の鍵または前記第1の鍵による暗号を復号化する復号化手段と、

前記暗号化手段により暗号化された暗号を他の情報処理装置に送信する送信手段と、

前記他の情報処理装置から暗号を受信する受信手段とを備える情報処理装置において、

前記所定のデータと、前記他の情報処理装置から受信した暗号を復号化して生成されたデータに応じて、前記他の情報処理装置を認証する認証手段をさらに備え、

前記暗号化手段が、前記第1の鍵で、第1のデータを第1の暗号に暗号化し、

前記送信手段が、前記第1の暗号を前記他の情報処理装置に送信し、

前記受信手段が、前記他の情報処理装置から、第2の暗号および第3の暗号を受け取り、

前記復号化手段が、前記第2の暗号を、前記第2の鍵で第4のデータに復号化するとともに、前記第3の暗号を、前記第2の鍵で第5のデータに復号化し、

前記認証手段が、前記第1のデータと前記第4のデータに応じて、前記他の情報処理装置を認証し、

前記暗号化手段が、前記第5のデータを、前記第1の鍵で第4の暗号に暗号化し、

前記送信手段が、前記第4の暗号を前記他の情報処理装置に送信することを特徴とする情報処理装置。

【請求項16】 前記第1のデータは、所定の認識番号であり、

前記第5のデータは、第3の鍵であり、

前記暗号化手段は、第1のコマンドを、前記第3の鍵で第5の暗号に暗号化するとともに、前記認識番号を、前記第3の鍵で第6の暗号に暗号化し、

前記送信手段は、前記第5の暗号を、前記第6の暗号とともに、前記他の情報処理装置に送信することを特徴とする請求項15に記載の情報処理装置。

【請求項17】 前記受信手段は、前記他の情報処理装置から前記第1のコマンドに対応する処理の結果に対応する応答データを暗号化した第7の暗号と、前記他の情報処理装置における前記認識番号を暗号化した第8の暗号を受信し、

前記復号化手段は、前記第7の暗号を、前記第3の鍵で第8のデータに復号化するとともに、前記第8の暗号を、前記第3の鍵で第9のデータに復号化し、

前記認証手段は、前記第9のデータと前記認識番号の値に応じて、前記第8のデータを、前記応答データとして承認することを特徴とする請求項16に記載の情報処理装置。

【請求項18】 前記認識番号は、前記第1のコマンドの暗号化毎に変更されることを特徴とする請求項16に記載の情報処理装置。

【請求項19】 前記認識番号は、前記第1のコマンドの暗号化毎に増加されることを特徴とする請求項18に記載の情報処理装置。

【請求項20】 前記認証手段は、前記第9のデータが前記認識番号に対応する所定の範囲内の値であるとき、前記第8のデータを、前記応答データとして承認することを特徴とする請求項17に記載の情報処理装置。

【請求項21】 前記認証手段は、前記第9のデータと前記認識番号の値を所定の桁数の範囲だけにおいて比較し、前記第9のデータにおける前記所定の桁数の範囲の値が、前記認識番号における前記所定の桁数の範囲の値以上であるとき、前記第8のデータを、前記応答データとして承認することを特徴とする請求項20に記載の情報処理装置。

【請求項22】 前記第5の暗号を、前記第6の暗号とともに送信した後、前記7の暗号および第8の暗号を受信するまでに所定の時間が経過した場合、前記認識番号の値を増加した後、前記認識番号を前記第6の暗号に暗号化し、前記第5の暗号を、前記第6の暗号とともに再送することを特徴とする請求項17に記載の情報処理装置。

【請求項23】 前記認証手段が前記第8のデータを応

答データとして承認しない場合、前記認識番号の値を増加した後、前記認識番号を前記第6の暗号に暗号化し、前記第5の暗号を、前記第6の暗号とともに再送することを特徴とする請求項17に記載の情報処理装置。

【請求項24】 第1の鍵および第2の鍵を記憶する記憶手段と、

所定のデータを、前記第1の鍵または前記第2の鍵を利用して暗号化する暗号化手段と、

前記第2の鍵または前記第1の鍵による暗号を復号化する復号化手段と、

前記暗号化手段により暗号化された暗号を他の情報処理装置に送信する送信手段と、

前記他の情報処理装置から暗号を受信する受信手段とを備える情報処理装置において、

前記所定のデータと、前記他の情報処理装置から受信した暗号を復号化して得られたデータに応じて、前記他の情報処理装置を認証する認証手段をさらに備え、

前記受信手段が、前記他の情報処理装置より第1の暗号を受け取り、

20 前記復号化手段が、前記第1の暗号を、前記第1の鍵で第2のデータに復号化し、

前記暗号化手段が、前記第2のデータを、前記第2の鍵で第2の暗号に暗号化するとともに、第3のデータを、前記第2の鍵で第3の暗号に暗号化し、

前記送信手段が、前記第2の暗号および前記第3の暗号を前記他の情報処理装置に送信し、

前記受信手段が、前記他の情報処理装置から第4の暗号を受け取り、

前記復号化手段が、前記第4の暗号を、前記第2の鍵で第6のデータに復号化し、

30 前記認証手段が、前記第3のデータと前記第6のデータに応じて、前記他の情報処理装置を認証することを特徴とする情報処理装置。

【請求項25】 前記第2のデータは、所定の認識番号であり、

前記第3のデータは、第3の鍵であり、

前記受信手段は、前記他の情報処理装置から、第1のコマンドを前記第3の鍵で暗号化した第5の暗号と、前記他の情報処理装置の前記認識番号を暗号化した第6の暗号を受信し、

40 前記復号化手段は、前記第5の暗号を、前記第3の鍵で第2のコマンドに復号化するとともに、前記第6の暗号を、前記第3の鍵で第7のデータに復号化し、

前記認証手段は、前記第7のデータと前記認識番号の値に応じて、前記第2のコマンドを承認することを特徴とする請求項24に記載の情報処理装置。

【請求項26】 前記第2のコマンドに対応する処理を行い、その処理の結果に対応する応答データを生成する処理手段をさらに備え、

50 前記暗号化手段は、前記応答データを、前記第3の鍵で

第7の暗号に暗号化するとともに、前記認識番号を、前記第3の鍵で第8の暗号に暗号化し、前記送信手段は、前記第7の暗号を、前記第8の暗号とともに送信することを特徴とする請求項25に記載の情報処理装置。

【請求項27】 前記認識番号は、前記第7の暗号の暗号化毎に変更されることを特徴とする請求項26に記載の情報処理装置。

【請求項28】 前記認識番号は、前記第7の暗号の暗号化毎に増加されることを特徴とする請求項27に記載の情報処理装置。

【請求項29】 前記認証手段は、前記第7のデータが、前記認識番号に対応する所定の範囲内の値であるとき、前記第2のコマンドを承認することを特徴とする請求項25に記載の情報処理装置。

【請求項30】 前記認証手段は、前記第7のデータと前記認識番号の値を所定の桁数の範囲だけにおいて比較し、前記第7のデータにおける前記所定の桁数の範囲の値が、前記認識番号における前記所定の桁数の範囲の値以上であるとき、前記第2のコマンドを承認することを特徴とする請求項25に記載の情報処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、認証方法、通信方法、および、情報処理装置に関し、特に、複数の情報処理装置が相互に認証を行う認証方法、通信方法、および、情報処理装置に関する。

【0002】

【従来の技術】情報処理技術の発展に伴い、大量の情報が所定の伝送路を介して通信されている。情報が通信される伝送路には、第三者（送信者および受信者以外の者）が、通信されているデータを盗聴することが可能なものが多い。

【0003】このような伝送路を利用して、情報を第三者に漏洩させずに、通信を行う場合、しばしば、暗号が利用される。暗号を利用し、暗号化されたデータを通信することにより、暗号化されたデータを盗聴することができても、第三者が、そのデータから通信した情報の内容を読み出すことは困難である。

【0004】このような暗号を生成する暗号化方法には、所定の鍵を利用して、平文（送信する情報）から、暗号（実際に送信されるデータ）を生成するものが利用されることが多い。

【0005】このような、鍵を利用した暗号には、共通鍵暗号と公開鍵暗号の2種類がある。共通鍵暗号においては、暗号化するときの鍵（暗号化鍵データ）と、復号化するときの鍵（復号化鍵データ）が同一である。例えば、共通鍵暗号としては、Feistel暗号の1つであるDES（Data Encryption Standard）方式などがよく利用されている。一方、公開鍵暗号においては、暗号化鍵デ

ータと復号化鍵データが異なる。そして、受信者は、送信者のために、それらの鍵のうち、暗号化鍵データを公開するが、復号化鍵データは公開せずに隠しておく（即ち、復号化鍵データは、受信者のみが知っている）。

【0006】図14は、このような鍵（共通鍵）を利用した通信（秘密通信）の一例を示している。送信者101は、送信する情報（平文M）を、鍵Kを利用して暗号Cに暗号化する。そして、送信者101は、暗号Cを、所定の伝送路を介して受信者102に送信する。

【0007】受信者102は、暗号Cを受け取り、送信者101が有する鍵Kと同一の鍵Kを利用して、その暗号Cを復号化し、送信者101により送信された情報（平文M）を獲得する。

【0008】このようにして通信が行われているとき、暗号Cを盗聴しても、第三者が、送信された情報（平文M）を獲得することは困難である。

【0009】さらに、このような鍵を利用して、通信相手が、正規の受信者であるか否かを判断する（認証する）ことができる。図15は、鍵（共通鍵）を利用した認証の一例を示している。認証する側111は、乱数Mを発生し、その乱数Mを認証される側112に送信する。認証する側111は、認証される側112に、その乱数Mを、鍵Kで暗号Cに暗号化させ、その暗号Cを送信させる。そして、認証する側111は、その暗号Cを受信し、鍵Kで平文M1に復号化する。そして、認証する側111は、乱数Mと平文M1が一致するか否かを判断し、一致する場合、認証される側112を認証する。

【0010】このようにして、送信者（認証する側111）は、受信者（認証される側112）が正規の受信者（送信者が有する鍵と同一の鍵を有する）であるか否かを判断する（認証する）ことができる。

【0011】このとき、平文である乱数Mと、それを暗号化した暗号Cを、第三者が盗聴したとしても、平文Mと暗号Cから、鍵Kを生成することは困難であるので、送信者（認証する側111）の鍵Kと同一の鍵Kを有する正規の受信者のみが認証される。

【0012】

【発明が解決しようとする課題】しかしながら、上述の認証方法においては、所定の送受信者が、他の送受信者を認証するだけであるので、例えば、リーダー/ライター（R/W）とICカードで構成されるカードシステムに、上述の認証方法を適用した場合、R/Wは、通信相手が正規のICカードであるか否かを判断する（通信相手を認証する）ことができるが、ICカードは、通信相手が正規のR/Wであるか否かを判断することが困難であるという問題を有している。

【0013】本発明は、このような状況に鑑みてなされたものであり、複数の情報処理装置において、相互に平文を送信するとともに、送信されてきた平文を受信し、受信した平文を暗号に暗号化し、平文を送信した装置

に、その暗号を送信するとともに、送信されてきた暗号を受信し、その暗号を復号化した平文と最初に送信した平文を比較することで、相互に認証を行うようにするものである。

#### 【0014】

【課題を解決するための手段】請求項1に記載の認証方法は、第1の情報処理装置の暗号化手段が、第1の鍵で、第1のデータを第1の暗号に暗号化するステップと、第2の情報処理装置の復号化手段が、第1の鍵で、第1の暗号を第2のデータに復号化するステップと、第2の情報処理装置の暗号化手段が、第2の鍵で、第2のデータを第2の暗号に暗号化するステップと、第2の情報処理装置の暗号化手段が、第2の鍵で、第3のデータを第3の暗号に暗号化するステップと、第1の情報処理装置の復号化手段が、第2の鍵で、第2の暗号を第4のデータに復号化するステップと、第1の情報処理装置が、第1のデータと第4のデータに応じて、第2の情報処理装置を認証するステップと、第1の情報処理装置の復号化手段が、第2の鍵で、第3の暗号を第5のデータに復号化するステップと、第1の情報処理装置の暗号化手段が、第1の鍵で、第5のデータを第4の暗号に暗号化するステップと、第2の情報処理装置の復号化手段が、第1の鍵で、第4の暗号を第6のデータに復号化するステップと、第2の情報処理装置が、第3のデータと第6のデータに応じて、第1の情報処理装置を認証するステップとを備えることを特徴とする。

【0015】請求項2に記載の通信方法は、第1の情報処理装置の暗号化手段が、第1の鍵で、第1のデータを第1の暗号に暗号化するステップと、第1の情報処理装置の送信手段が、第1の暗号を、第2の情報処理装置に送信するステップと、第2の情報処理装置の受信手段が、第1の暗号を受信するステップと、第2の情報処理装置の復号化手段が、第1の鍵で、第1の暗号を第2のデータに復号化するステップと、第2の情報処理装置の暗号化手段が、第2の鍵で、第2のデータを第2の暗号に暗号化するステップと、第2の情報処理装置の暗号化手段が、第2の鍵で、第3のデータを第3の暗号に暗号化するステップと、第2の情報処理装置の送信手段が、第2の暗号および第3の暗号を、第1の情報処理装置に送信するステップと、第1の情報処理装置の受信手段が、第2の暗号および第3の暗号を受信するステップと、第1の情報処理装置の復号化手段が、第2の鍵で、第2の暗号を第4のデータに復号化するステップと、第1の情報処理装置が、第1のデータと第4のデータに応じて、第2の情報処理装置を認証するステップと、第1の情報処理装置の復号化手段が、第2の鍵で、第3の暗号を第5のデータに復号化するステップと、第1の情報処理装置の暗号化手段が、第1の鍵で、第5のデータを第4の暗号に暗号化するステップと、第1の情報処理装置の送信手段が、第4の暗号を、第2の情報処理装置に

送信するステップと、第2の情報処理装置の受信手段が、第4の暗号を受信するステップと、第2の情報処理装置の復号化手段が、第1の鍵で、第4の暗号を第6のデータに復号化するステップと、第2の情報処理装置が、第3のデータと第6のデータに応じて、第1の情報処理装置を認証するステップとを備えることを特徴とする。

【0016】請求項15に記載の情報処理装置は、所定のデータと、他の情報処理装置から受信した暗号を復号化して生成されたデータに応じて、他の情報処理装置を認証する認証手段をさらに備え、暗号化手段が、第1の鍵で、第1のデータを第1の暗号に暗号化し、送信手段が、第1の暗号を他の情報処理装置に送信し、受信手段が、他の情報処理装置から、第2の暗号および第3の暗号を受け取り、復号化手段が、第2の暗号を、第2の鍵で第4のデータに復号化するとともに、第3の暗号を、第2の鍵で第5のデータに復号化し、認証手段が、第1のデータと第4のデータに応じて、他の情報処理装置を認証し、暗号化手段が、第5のデータを、第1の鍵で第4の暗号に暗号化し、送信手段が、第4の暗号を他の情報処理装置に送信することを特徴とする。

【0017】請求項24に記載の情報処理装置は、所定のデータと、他の情報処理装置から受信した暗号を復号化して得られたデータに応じて、他の情報処理装置を認証する認証手段をさらに備え、受信手段が、他の情報処理装置により第1の暗号を受け取り、復号化手段が、第1の暗号を、第1の鍵で第1のデータに復号化し、暗号化手段が、第1のデータを、第2の鍵で第2の暗号に暗号化するとともに、第2のデータを、第2の鍵で第3の暗号に暗号化し、送信手段が、第2の暗号および第3の暗号を他の情報処理装置に送信し、受信手段が、他の情報処理装置から第4の暗号を受け取り、復号化手段が、第4の暗号を、第2の鍵で第3のデータに復号化し、認証手段が、第2のデータと第3のデータに応じて、他の情報処理装置を認証することを特徴とする。

【0018】請求項1に記載の認証方法においては、第1の情報処理装置の暗号化手段が、第1の鍵で、第1のデータを第1の暗号に暗号化し、第2の情報処理装置の復号化手段が、第1の鍵で、第1の暗号を第2のデータに復号化し、第2の情報処理装置の暗号化手段が、第2の鍵で、第2のデータを第2の暗号に暗号化し、第2の情報処理装置の暗号化手段が、第2の鍵で、第3のデータを第3の暗号に暗号化し、第1の情報処理装置の復号化手段が、第2の鍵で、第2の暗号を第4のデータに復号化し、第1の情報処理装置が、第1のデータと第4のデータに応じて、第2の情報処理装置を認証し、第1の情報処理装置の復号化手段が、第2の鍵で、第3の暗号を第5のデータに復号化し、第1の情報処理装置の暗号化手段が、第1の鍵で、第5のデータを第4の暗号に暗号化し、第2の情報処理装置の復号化手段が、第1の鍵

で、第4の暗号を第6のデータに復号化し、第2の情報処理装置が、第3のデータと第6のデータに応じて、第1の情報処理装置を認証する。

【0019】請求項2に記載の通信方法においては、第1の情報処理装置の暗号化手段が、第1の鍵で、第1のデータを第1の暗号に暗号化し、第1の情報処理装置の送信手段が、第1の暗号を、第2の情報処理装置に送信し、第2の情報処理装置の受信手段が、第1の暗号を受信し、第2の情報処理装置の復号化手段が、第1の鍵で、第1の暗号を第2のデータに復号化し、第2の情報処理装置の暗号化手段が、第2の鍵で、第2のデータを第2の暗号に暗号化し、第2の情報処理装置の暗号化手段が、第2の鍵で、第3のデータを第3の暗号に暗号化し、第2の情報処理装置の送信手段が、第2の暗号および第3の暗号を、第1の情報処理装置に送信し、第1の情報処理装置の受信手段が、第2の暗号および第3の暗号を受信し、第1の情報処理装置の復号化手段が、第2の鍵で、第2の暗号を第4のデータに復号化し、第1の情報処理装置が、第1のデータと第4のデータに応じて、第2の情報処理装置を認証し、第1の情報処理装置の復号化手段が、第2の鍵で、第3の暗号を第5のデータに復号化し、第1の情報処理装置の暗号化手段が、第1の鍵で、第5のデータを第4の暗号に暗号化し、第1の情報処理装置の送信手段が、第4の暗号を、第2の情報処理装置に送信し、第2の情報処理装置の受信手段が、第4の暗号を受信し、第2の情報処理装置の復号化手段が、第1の鍵で、第4の暗号を第6のデータに復号化し、第2の情報処理装置が、第3のデータと第6のデータに応じて、第1の情報処理装置を認証する。

【0020】請求項15に記載の情報処理装置においては、暗号化手段が、第1の鍵で、第1のデータを第1の暗号に暗号化し、送信手段が、第1の暗号を他の情報処理装置に送信し、受信手段が、他の情報処理装置から、第2の暗号および第3の暗号を受け取り、復号化手段が、第2の暗号を、第2の鍵で第4のデータに復号化するとともに、第3の暗号を、第2の鍵で第5のデータに復号化し、認証手段が、第1のデータと第4のデータに応じて、他の情報処理装置を認証し、暗号化手段が、第5のデータを、第1の鍵で第4の暗号に暗号化し、送信手段が、第4の暗号を他の情報処理装置に送信する。

【0021】請求項24に記載の情報処理装置においては、受信手段が、他の情報処理装置により第1の暗号を受け取り、復号化手段が、第1の暗号を、第1の鍵で第1のデータに復号化し、暗号化手段が、第1のデータを、第2の鍵で第2の暗号に暗号化するとともに、第2のデータを、第2の鍵で第3の暗号に暗号化し、送信手段が、第2の暗号および第3の暗号を他の情報処理装置に送信し、受信手段が、他の情報処理装置から第4の暗号を受け取り、復号化手段が、第4の暗号を、第2の鍵で第3のデータに復号化し、認証手段が、第2のデータ

と第3のデータに応じて、他の情報処理装置を認証する。

【0022】

【発明の実施の形態】図1は、R/W1およびICカード2を利用した非接触カードシステムの一例を示している。R/W1およびICカード2は、電磁波を利用して非接触で、データの送受信を行う。

【0023】例えば、R/W1が、リードコマンドをICカード2に送信すると、ICカード2は、そのリードコマンドを受信し、リードコマンドで指示されたデータをR/W1に送信するようになされている。

【0024】また、R/W1がデータをICカード2に送信すると、ICカード2は、そのデータを受信し、受信したデータを、内蔵するメモリ84（図6）（記憶手段）に記憶し、そのデータを記憶したことを表す所定の応答信号をR/W1に送信するようになされている。

【0025】図2は、本発明の一実施例であるR/W1の構成を示している。

【0026】R/W1においては、制御部11は、内蔵するプログラムに応じて、各種処理を行うようになされている。例えば、制御部11は、ICカード2に送信するデータを、暗号部12（暗号化手段）に出力するとともに、復号部13（復号化手段）より供給された、ICカード2からの応答データを処理するようになされている。

【0027】また、制御部11は、メモリ14（記憶手段）から、暗号化または復号化に利用される鍵K<sub>a</sub>（第2の鍵）または鍵K<sub>b</sub>（第1の鍵）を読み出し、その鍵K<sub>a</sub>または鍵K<sub>b</sub>を、暗号部12または復号部13に出力するようになされている。

【0028】さらに、制御部11は、インタフェース15を介して、メインコンピュータ（図示せず）と通信を行うようになされている。

【0029】メモリ14は、制御部11における処理に使用されるデータなどを記憶している他、暗号化または復号化において利用される2つの鍵K<sub>a</sub>、K<sub>b</sub>を記憶している。

【0030】暗号部12は、制御部11より供給されたデータを、所定の鍵で暗号化し、暗号化したデータ（暗号）を送信部16（送信手段）に出力するようになされている。

【0031】送信部16は、暗号部12より供給されたデータ（暗号）を、所定の変調方式（例えば、PSK（Phase Shift Keying）変調方式）で変調し、生成された変調波を、アンテナ部17を介してICカード2に送信するようになされている。

【0032】受信部18（受信手段）は、アンテナ部17を介して、ICカード2により送信された変調波を受信し、その変調波に対応する復調方式で復調し、復調したデータ（暗号）を復号部13に出力するようになされ



ている。

【0033】復号部13は、受信部18より供給されたデータ（暗号）を、所定の鍵で復号化し、復号化したデータを制御部11に出力するようになされている。

【0034】図3は、図2の暗号部12の一構成例を示している。暗号部12においては、鍵保存部31は、制御部11より供給された鍵Kを保持するようになされている。

【0035】データランダム化部32は、鍵保存部31から鍵Kを読み出し、その鍵Kで、制御部31より供給されたデータを暗号化し、生成された暗号を送信部16に出力するようになされている。

【0036】図4は、図3のデータランダム化部32の一構成例を示している。このデータランダム化部32は、複数のインポリューション処理を行うDES方式（例えば、「暗号と情報セキュリティ」辻井 重男、笠原 正雄 編著、1990年、昭晃堂に記載されている）で暗号を生成するようになされている。このデータランダム化部32においては、鍵データ生成回路61は、鍵保存部31から読み出した鍵Kから、16個の鍵データ $K_1$ 乃至 $K_{16}$ を算出し、鍵データ $K_1$ 乃至 $K_{16}$ を、演算回路62-1乃至62-16にそれぞれ出力するようになされている。

【0037】レジスタ63は、制御部11より供給された64ビット（8バイト）のデータを保持し、その64ビットのデータのうちの上位32ビットを加算器64-1に出力し、下位32ビットを演算回路62-1および加算器64-2に出力するようになされている。

【0038】演算回路62-i（ $i=1, \dots, 16$ ）は、レジスタ63の下位32ビット（演算回路62-1の場合）または加算器64-（ $i-1$ ）（演算回路62-2乃至62-16の場合）より供給された32ビットのデータに対して、鍵データ生成回路61より供給された鍵データ $K_i$ を利用して、所定の変換を行い、変換後の32ビットのデータを加算器64-iに出力するようになされている。

【0039】加算器64-i（ $i=1, \dots, 16$ ）は、レジスタ63の上位32ビット（加算器64-1の場合）、レジスタ63の下位32ビット（加算器64-2の場合）、および、加算器64-（ $i-2$ ）（加算器64-3乃至64-16の場合）のいずれかより供給された32ビットのデータと、演算回路62-iより供給された32ビットのデータの排他的論理和（ビット毎の排他的論理和）を計算し、その排他的論理和（32ビット）を、加算器64-（ $i+2$ ）（加算器64-1乃至64-14の場合）、レジスタ65の下位32ビット（加算器64-15の場合）、および、レジスタ65の上位32ビット（加算器64-16の場合）のいずれか、並びに、演算回路62-（ $i+1$ ）（加算器64-1乃至64-15の場合）に出力するようになされてい

る。

【0040】レジスタ65は、加算器64-15より供給された32ビットのデータを、下位32ビットで保持し、加算器64-16より供給された32ビットのデータを、上位32ビットで保持するとともに、これらの2つの32ビットのデータで構成される64ビットのデータを、暗号として送信部16に出力するようになされている。

【0041】図5は、図2の復号部13の一構成例を示している。この復号部13においては、鍵保存部41は、制御部11より供給された鍵Kを保持するようになされている。

【0042】変換部42は、図4のデータランダム化部32と同一の構成を有し、鍵保存部41から鍵Kを読み出し、受信部18より供給されたデータ（DES方式で暗号化された暗号）をレジスタ63に供給した後、図4のデータランダム化部32と同一の動作を行い、そのデータを復号化し、復号化したデータをレジスタ65から制御部11に出力するようになされている。

【0043】図6は、本発明の一実施例であるICカード2の構成例を示している。

【0044】ICカード2においては、制御部81（処理手段）は、R/W1により供給されるコマンドに応じて、各種処理を行うようになされている。制御部81は、R/W1からのコマンドを、復号部83（復号化手段）から受け取り、そのコマンドに対応した処理を行い、その処理の結果に対応する応答データ（R/W1に送信するもの）を、暗号部82（暗号化手段）に出力するようになされている。

【0045】また、制御部81は、メモリ84から、暗号化または復号化に利用される鍵 $K_A$ または鍵 $K_B$ を読み出し、その鍵 $K_A$ または鍵 $K_B$ を、暗号部82または復号部83に出力するようになされている。

【0046】メモリ84は、RAM（Random Access Memory）部（128キロバイト程度）とROM（Read Only Memory）部（512キロバイト程度）を有している。そのうちのRAM部は、制御部81における処理に使用されるデータなどを一時的に記憶する。一方、ROM部には、暗号化または復号化において利用される2つの鍵 $K_A$ 、 $K_B$ が、予め記憶されている。

【0047】暗号部82および復号部83は、図3の暗号部12および図5の復号部13と同様の構成であるので、その説明を省略する。

【0048】送信部86（送信手段）は、暗号部82より供給されたデータ（暗号）を、所定の変調方式（例えば、PSK（Phase Shift Keying）変調方式）で変調し、生成された変調波を、アンテナ部87を介してR/W1に送信するようになされている。

【0049】受信部88（受信手段）は、アンテナ部87を介して、R/W1により送信された変調波を受信

し、その変調波に対応する復調方式で復調し、復調したデータ（暗号）を復号部83に出力するようになされている。

【0050】次に、図7および図8のフローチャート、並びに、図9を参照して、R/W1とICカード2の、相互認証を行うときの動作について説明する。

【0051】最初に図7のステップS1において、R/W1の制御部11は、64ビットの乱数R<sub>A</sub>（第1のデータ）を生成し、その乱数R<sub>A</sub>を暗号部12のデータランダム化部32に出力するとともに、メモリ14から鍵K<sub>A</sub>を読み出し、暗号部12の鍵保存部31に出力する。

【0052】図3の暗号部12のデータランダム化部32は、鍵保存部31から鍵K<sub>A</sub>を読み出す。そして、図4のデータランダム化部32の鍵データ生成回路61は、鍵K<sub>A</sub>から16個の鍵データK<sub>1</sub>乃至K<sub>16</sub>を生成し、演算回路62-1乃至62-16にそれぞれ出力する。

【0053】データランダム化部32のレジスタ63は、R/W1より供給された乱数R<sub>A</sub>の上位32ビットを加算器64-1に出力し、乱数R<sub>A</sub>の下位32ビットを演算回路62-1および加算器64-2に出力する。演算回路62-1は、その32ビットのデータを鍵データK<sub>1</sub>を利用して変換し、変換後のデータを加算器64-1に出力する。加算器64-1は、レジスタ63より供給された32ビットのデータと、演算回路62-1より供給された32ビットのデータの排他的論理和（ビット毎の排他的論理和）を計算し、その排他的論理和（32ビット）を、演算回路62-2および加算器64-3に出力する。

【0054】次に、演算回路62-2は、その32ビットのデータを鍵データK<sub>2</sub>を利用して変換し、変換後のデータ（32ビット）を加算器64-2に出力する。加算器64-2は、レジスタ63より供給された32ビットのデータと、演算回路62-2より供給された32ビットのデータの排他的論理和を計算し、その排他的論理和を、演算回路62-3および加算器64-4に出力する。

【0055】演算回路62-3乃至62-14および加算器64-3乃至64-14は、順次、演算回路62-2および加算器64-2と同様の動作を行う。即ち、演算回路62-j（j=3, ..., 14）は、加算器64-(j-1)より供給された32ビットのデータを鍵データK<sub>j</sub>を利用して変換し、変換後のデータを加算器64-jに出力する。加算器64-j（j=3, ..., 14）は、加算器64-(j-2)より供給された32ビットのデータと、演算回路62-jより供給された32ビットのデータの排他的論理和を計算し、その排他的論理和を、演算回路62-(j+1)および加算器64-(j+2)に出力する。

【0056】さらに、演算回路62-15は、加算器6

4-14より供給された32ビットのデータを鍵データK<sub>15</sub>を利用して変換し、変換後のデータを加算器64-15に出力する。加算器64-15は、加算器64-13より供給された32ビットのデータと、演算回路62-15より供給された32ビットのデータの排他的論理和を計算し、その排他的論理和を、演算回路62-16およびレジスタ65の下位32ビットに出力する。

【0057】そして、演算回路62-16は、その32ビットのデータを鍵データK<sub>16</sub>を利用して変換し、変換後のデータを加算器64-16に出力する。加算器64-16は、加算器64-14より供給された32ビットのデータと、演算回路62-16より供給された32ビットのデータの排他的論理和を計算し、その排他的論理和を、レジスタ65の上位32ビットに出力する。

【0058】以上のようにして、合計16段の演算を行って暗号を生成する。そして、データランダム化部32のレジスタ65は、生成した暗号C<sub>1</sub>（第1の暗号）（図9の[R<sub>A</sub>]<sub>a</sub>）を送信部16に出力する。

【0059】次に、ステップS2において、R/W1の送信部16は、暗号部12より供給された暗号C<sub>1</sub>を変調し、生成された変調波を、アンテナ部17を介してICカード2に送信する。

【0060】このように、R/W1が、ステップS1、S2において処理を行い、変調波を送信するまでの間、ICカード2は、図8のステップS21において待機している。

【0061】そして、R/W1から変調波が送信されてくると、ICカード2の受信部88は、アンテナ部87を介して、R/W1の送信部16により送信された変調波を受信し、その変調波を復調し、復調後のデータ（暗号C<sub>1</sub>）を復号部83に出力する。

【0062】次に、ステップS22において、ICカード2の復号部83の変換部42は、予め制御部81より鍵保存部41に供給されている鍵K<sub>A</sub>で、受信部88より供給された暗号C<sub>1</sub>を復号化し、復号化したデータ（平文M<sub>1</sub>）（第2のデータ）を制御部81に出力する。

【0063】ステップS23において、ICカード2の制御部81は、復号部83より供給された平文M<sub>1</sub>を、暗号部82のデータランダム化部32に出力する。暗号部82のデータランダム化部32は、鍵保存部31に予め記憶されている鍵K<sub>A</sub>を読み出し、その鍵K<sub>A</sub>で、ステップS1におけるR/W1の暗号部12のデータランダム化部32と同様に、平文M<sub>1</sub>を暗号化し、生成された暗号C<sub>2</sub>（第2の暗号）（図9の[R<sub>A</sub>]<sub>a</sub>）を送信部86に出力する。

【0064】また、制御部81は、乱数R<sub>B</sub>（第3のデータ）を生成し、その乱数R<sub>B</sub>を暗号部82のデータランダム化部32に出力する。暗号部82のデータランダム化部32は、鍵保存部31から鍵K<sub>A</sub>を読み出し、そ

17

の鍵 $K_A$ で乱数 $R_B$ を暗号化し、生成された暗号 $C_1$ （第3の暗号）（図9の $[R_B]_A$ ）を送信部86に出力する。

【0065】そして、ステップS24において、ICカード2の送信部86は、暗号 $C_2$ 、 $C_3$ を変調し、生成された変調波を、アンテナ部87を介してR/W1に送信する。

【0066】このように、ICカード2がステップS21乃至S24の処理を行っている間、R/W1は、図7のステップS3およびステップS4において、ICカード2から暗号 $C_2$ と暗号 $C_3$ が送信されてくるまで待機するとともに、暗号 $C_1$ を送信してから経過時間を、ステップS3において監視し、ICカード2から $C_2$ と $C_3$ が送信されてくるまでに所定の時間（ICカード2における処理に通常要する時間より長い時間）が経過した場合、ステップS2に戻り、暗号 $C_1$ を再送する。

【0067】そして、ICカード2から暗号 $C_2$ および暗号 $C_3$ を含む変調波が送信されてくると、R/W1に受信部18は、アンテナ部17を介して、ICカード2の送信部86により送信された変調波を受信し、その変調波を復調する。そして、受信部18は、復調されたデータ（暗号 $C_2$ 、 $C_3$ ）を、復号部13に出力する。

【0068】次に、ステップS5において、R/W1の復号部13の変換部42は、鍵保存部41に予め供給されている鍵 $K_A$ を読み出し、受信部18より供給されたデータ（暗号 $C_2$ 、 $C_3$ ）を復号化し、復号化したデータ（平文 $M_2$ （暗号 $C_2$ に対応する）（第4のデータ）と平文 $M_3$ （暗号 $C_3$ に対応する）（第5のデータ））を制御部11に出力する。

【0069】そして、ステップS6において、R/W1の制御部11は、平文 $M_2$ と乱数 $R_A$ が同一であるか否かを判断し、平文 $M_2$ と乱数 $R_A$ が同一であると判断した場合、ステップS7において、R/W1は、ICカード2がR/W1の鍵 $K_A$ 、 $K_B$ と同一の鍵 $K_A$ 、 $K_B$ を有していると判断し、ICカード2を認証する。

【0070】一方、ステップS6において、平文 $M_2$ と乱数 $R_A$ が同一ではないと判断した場合、R/W1は、ICカード2を認証しないので、認証処理を終了する。

【0071】ステップS7においてICカード2を認証した後、ステップS8において、R/W1の制御部11は、ステップS5で生成した平文 $M_3$ を暗号部12に出力する。そして、暗号部12は、ステップS1と同様に、平文 $M_3$ を鍵 $K_B$ で暗号化し、生成された暗号 $C_4$ （第4の暗号）（図9の $[R_B]_B$ ）を送信部16に出力する。

【0072】ステップS9において、R/W1の送信部16は、暗号部12より供給された暗号 $C_4$ を変調し、生成された変調波を、アンテナ部17を介してICカード2に送信する。

【0073】このように、R/W1が、ステップS4乃

18

至S9において処理を行っている間、ICカード2は、図8のステップS25およびステップS26において、暗号 $C_4$ が送信されてくるまで待機している。このとき、ICカード2の制御部81は、暗号 $C_2$ 、 $C_3$ を送信してから経過時間を監視しており、ステップS26において暗号 $C_2$ 、 $C_3$ を送信してから所定の時間が経過したと判断した場合、R/W1を認証せずに認証処理を終了する。

【0074】一方、暗号 $C_4$ を含む変調波が送信されてくると、ICカード2の受信部88は、R/W1により送信された変調波を、アンテナ部87を介して受信し、その変調波を復調する。そして、受信部88は、復調したデータ（暗号 $C_4$ ）を復号部13に出力する。

【0075】次にステップS27において、ICカード2の復号部83の変換部42は、鍵保存部41から読み出した鍵 $K_B$ で、受信部88より供給されたデータ（暗号 $C_4$ ）を復号化し、復号化したデータ（平文 $M_4$ ）（第6のデータ）を制御部81に出力する。

【0076】そして、ステップS28において、ICカード2の制御部81は、平文 $M_4$ と乱数 $R_B$ が同一であるか否かを判断し、平文 $M_4$ と乱数 $R_B$ が同一であると判断した場合、ステップS29において、ICカード2は、R/W1がICカード2の鍵 $K_A$ 、 $K_B$ と同一の鍵 $K_A$ 、 $K_B$ を有していると判断し、R/W1を認証する。

【0077】一方、ステップS28において、平文 $M_4$ と乱数 $R_B$ が同一ではないと判断した場合、ICカード2は、R/W1を認証しないので、認証処理を終了する。

【0078】以上のようにして、R/W1は、図7に示すように、ICカード2に対する認証処理を行い、ICカード2は、図8に示すように、R/W1に対する認証処理を行うことにより、相互に、認証処理を行う。

【0079】なお、上述の暗号部12、82のデータランダム化部32は、DES方式で暗号化を行っているが、他の方式（例えば、FEAL（Fast Encryption Algorithm）－8方式）で暗号化を行うようにしてもよい。その場合、復号部13、83の変換部42は、その暗号化方式に対応して復号化を行うようにする。

【0080】また、FEAL－8方式を利用した場合、35ミリ秒程度（ICカード2における処理にかかる時間は28ミリ秒程度）で相互認証を行うことができる。

【0081】次に、図10および図11のフローチャートを参照して、上述の認証処理後（相互に認証した後）におけるR/W1とICカード2間の通信について説明する。

【0082】図10のステップS41において、R/W1の制御部11は、最初に、上述の認証処理における乱数 $R_A$ を認識番号IDとして保持するとともに、乱数 $R_B$ （平文 $M_3$ ）（ICカード2を認証したので、R/W1は、平文 $M_3$ を乱数 $R_B$ とする）を新たな鍵 $K_{10}$ （第3の

鍵)として、暗号部12の鍵保存部31および復号部13の鍵保存部41に出力する。

【0083】そして、R/W1の制御部11は、ICカード2に実行させる処理に対応するコマンド(送信コマンド)を、暗号部12のデータランダム化部32に出力する。暗号部12のデータランダム化部32は、鍵保存部31から鍵K<sub>10</sub>を読み出し、その鍵K<sub>10</sub>で送信コマンドを暗号化し、生成された暗号C<sub>com</sub>(第5の暗号)を送信部16に出力する。

【0084】また、R/W1の制御部11は、認識番号IDを、暗号部12のデータランダム化部32に出力する。暗号部12のデータランダム化部32は、鍵K<sub>10</sub>で認識番号IDを暗号化し、生成された暗号C<sub>10</sub>(第6の暗号)を送信部16に出力する。

【0085】ステップS42において、R/W1の送信部16は、暗号部12より供給された暗号C<sub>com</sub>、C<sub>10</sub>を変調し、生成された変調波をアンテナ部17を介してICカード2に送信する。

【0086】このように、R/W1が、暗号C<sub>com</sub>、C<sub>10</sub>を含む変調波を送信するまでの間、ICカード2は、図11のステップS61において待機している。

【0087】なお、ICカード2の制御部81は、上述の認証処理における乱数R<sub>a</sub>を鍵K<sub>10</sub>として、予め、暗号部82の鍵保存部31および復号部83の鍵保存部41に出力するとともに、乱数R<sub>a</sub>(平文M<sub>1</sub>)(R/W1を認証したので、ICカード2は、平文M<sub>1</sub>を乱数R<sub>a</sub>とする)を認識番号IDとして保持している。

【0088】そして、R/W1から暗号C<sub>com</sub>、C<sub>10</sub>を含む変調波を送信されてくると、ICカード2の受信部88は、R/W1の送信部16により送信された変調波を、アンテナ部87を介して受信し、その変調波を復調する。そして、受信部88は、復調したデータ(暗号C<sub>com</sub>、C<sub>10</sub>)を、復号部83に出力する。

【0089】ステップS62において、復号部83の変換部42は、鍵保存部41に予め記憶されている鍵K<sub>10</sub>で、供給されたデータのうちの暗号C<sub>10</sub>を復号化し、復号されたデータ(平文M<sub>10</sub>)(第7のデータ)を制御部81に出力する。

【0090】そして、ステップS63において、ICカード2の制御部81は、平文M<sub>10</sub>の値が認識番号ID以上であるか否かを判断し、平文M<sub>10</sub>の値が認識番号IDより小さいと判断した場合、通信処理を終了する。一方、平文M<sub>10</sub>の値が認識番号ID以上であると判断した場合、ステップS64において、制御部81は、送信されてきたコマンド(暗号C<sub>com</sub>)を承認し、復号部83に、暗号C<sub>com</sub>を復号化させ、ステップS65において、復号化したコマンドに対応する処理を行い、ステップS66において、その処理結果に対応する応答データ(R/W1に送信するためのもの)を作成する。

【0091】次に、ステップS67において、ICカー

ド2の制御部81は、認識番号IDの値を1だけ増加させた後、認識番号IDおよび応答データを、暗号部82に順次出力する。ステップS68において、暗号部82は、認識番号IDを、鍵K<sub>10</sub>で暗号C<sub>10</sub>(第8の暗号)に暗号化するとともに、応答データを、鍵K<sub>10</sub>で暗号C<sub>re</sub>(第7の暗号)に暗号化した後、暗号C<sub>10</sub>および暗号C<sub>re</sub>を、送信部86に出力する。

【0092】そして、ステップS69において、送信部86は、暗号C<sub>10</sub>と暗号C<sub>re</sub>を変調し、生成した変調波をR/W1に送信する。

【0093】このように、ICカード2がステップS61乃至S69において送信したコマンドに対応する処理を行っている間、R/W1は、ステップS43およびステップS44において待機するとともに、暗号C<sub>10</sub>、C<sub>com</sub>を送信した時からの経過時間をステップS43において監視する。

【0094】そして、予め設定されている所定の時間が経過すると、ステップS45に進み、制御部11は、ステップS41で暗号化したコマンドと同一のコマンドを選択し、ステップS46で、認識番号IDの値を1だけ増加させた後、ステップS41に戻り、送信コマンドと認識番号IDを暗号化し、ステップS42において、生成された暗号をICカード2に再送する。

【0095】一方、ステップS44において、ICカード2からの暗号C<sub>10</sub>と暗号C<sub>re</sub>を含む変調波が送信されてくると、R/W1に受信部18が、その変調波を、暗号C<sub>10</sub>と暗号C<sub>re</sub>に復調し、その暗号C<sub>10</sub>と暗号C<sub>re</sub>を復号部13に出力する。

【0096】ステップS47において、復号部13は、暗号C<sub>10</sub>を鍵K<sub>10</sub>で復号化し、生成された平文M<sub>10</sub>(第9のデータ)を制御部11に出力する。

【0097】ステップS48において、制御部11は、平文M<sub>10</sub>の値が、認識番号IDより大きいかなかを判断し、平文M<sub>10</sub>の値が認識番号ID以下であると判断した場合、ステップS45に進み、ステップS41で送信したコマンドと同一のコマンドを選択し、ステップS46において、認識番号IDの値を1だけ増加させた後、ステップS41に戻り、送信コマンドと認識番号IDを暗号化し、ステップS42において、生成された暗号をICカード2に再送する。

【0098】一方、ステップS48において、平文M<sub>10</sub>の値が、認識番号IDより大きいと判断した場合、制御部11は、ステップS49において、復号部13に、暗号C<sub>re</sub>を復号化させ、ICカード2からの応答データを受け取る。

【0099】そして、ステップS50において、R/W1の制御部11は、通信を終了するか否かを判断する。通信を継続する場合、ステップS51に進み、R/W1の制御部11は、次の送信コマンドを選択する。

【0100】そして、ステップS46に進み、認識番号

IDの値を1だけ増加させた後、ステップS41に戻り、ステップS41以降で、次の送信コマンドの送信を行う。

【0101】以上のようにして、相互認証時に送信した乱数 $R_A$ 、 $R_B$ を、認識番号IDおよび新たな鍵 $K_{10}$ として利用して、R/W1は、ICカード2に所定のコマンドを送信し、ICカード2は、そのコマンドに対応する処理を行った後、その処理結果に対応する応答データをR/W1に送信する。このようにすることにより、認識番号および新たな鍵を利用して、通信毎に、通信相手が正規の者であることを確認することができる。また、1回の通信毎に認識番号IDの値を1ずつ増加させているので、現在までの通信回数を知ることができ、処理の経過を把握することができる。

【0102】なお、ステップS63において、ICカード2の制御部81は、平文 $M_{10}$ が認識番号ID以上であるか否かを判断しているが、平文 $M_{10}$ の値が認識番号IDに対応する所定の範囲内（例えば、ID乃至ID+16の範囲）の値と同一であるか否かを判断するようにしてもよい。このようにすることにより、例えば、伝送路に障害が生じ、R/W1が放射した電磁波（認識番号の値がID）がICカード2に到達しなかった場合において、ICカード2は、次に送信されてくるデータ（認識番号の値はID+1であるが、送信コマンドは、前回送信したコマンドと同一である）を受信することができる。

【0103】あるいは、ステップS63において、ICカード2の制御部81は、平文 $M_{10}$ （64ビット）の例えば下位8ビットの値が、認識番号IDの下位8ビットの値以上であるか否かを判断するようにしてもよい。このように所定の桁数（ビット数） $n$ だけにおいて比較を行うことにより、64ビットにおいて比較を行う場合より、ビット演算量が減少し、処理を速く行うことができる。なお、この場合、認識番号IDの値が $2^n - 1$ （ $n$ は桁数）より大きくなると桁上がりが発生する（比較の結果にエラーが生じる）ので、R/W1とICカード2の間の通信の回数を考慮して、認識番号IDの値が $2^n - 1$ （ $n$ は桁数）より大きくならないように、桁数 $n$ を設定する。

【0104】また、同様に、ステップS48において、R/W1の制御部11は、平文 $M_{10}$ の値が認識番号IDに対応する所定の範囲内の値と同一であるか否かを判断するようにしてもよい。また、ステップS48において、R/W1の制御部11は、平文 $M_{10}$ の例えば下位8ビットの値が、認識番号IDの下位8ビットの値より大きいかな否かを判断するようにしてもよい。

【0105】なお、上記実施例においては、乱数 $R_B$ を新たな鍵 $K_{10}$ としているが、図12に示すように乱数 $R_A$ と乱数 $R_B$ から新たな鍵 $K_{10}$ を算出し、その鍵 $K_{10}$ を利用して通信を行うようにしてもよい。

【0106】また、R/W1が送信した情報を、ICカード2に、単に記憶しておく場合、図13に示すように、ICカード2は、受信したデータ（鍵 $K_A$ または鍵 $K_B$ で暗号化されたデータ）を、復号化せずに、そのままメモリ84に記憶させておき、R/W1からのリードコマンドを受け取ったときに、そのデータをメモリ84から読み出し、そのまま送信するようにしてもよい。

【0107】

【発明の効果】以上のごとく、請求項1に記載の認証方法によれば、第1の情報処理装置が、第1のデータを第1の暗号に暗号化し、第2の情報処理装置が、第1の暗号を第2のデータに復号化し、その第2のデータを第2の暗号に暗号化するとともに、第3のデータを第3の暗号に暗号化し、第1の情報処理装置が、第2の暗号を第4のデータに復号化し、第1の情報処理装置が、第1のデータと第4のデータに応じて、第2の情報処理装置を認証する。そして、第1の情報処理装置が、第3の暗号を第5のデータに復号化し、その第5のデータを第4の暗号に暗号化し、第2の情報処理装置が、第4の暗号を第6のデータに復号化し、第2の情報処理装置が、第3のデータと第6のデータに応じて、第1の情報処理装置を認証するようにしたので、2つの情報処理装置が相互に認証を行うことができる。

【0108】請求項2に記載の通信方法によれば、第1の情報処理装置が、第1のデータを暗号化した第1の暗号を、第2の情報処理装置に送信し、第2の情報処理装置が、第1の暗号を受信し、その第1の暗号を第2のデータに復号化するとともに、その第2のデータを暗号化した第2の暗号と、第3のデータを暗号化した第3の暗号を、第1の情報処理装置に送信し、第1の情報処理装置が、第2の暗号および第3の暗号を受信し、そのうちの第2の暗号を第4のデータに復号化し、第1の情報処理装置が、第1のデータと第4のデータに応じて、第2の情報処理装置を認証する。そして、第1の情報処理装置が、第3の暗号を第5のデータに復号化するとともに、第5のデータを暗号化した第4の暗号を、第2の情報処理装置に送信し、第2の情報処理装置が、第4の暗号を受信し、その第4の暗号を第6のデータに復号化するとともに、第3のデータと第6のデータに応じて、第1の情報処理装置を認証するようにしたので、相互に認証した2つの情報処理装置で通信を行うことができる。

【0109】請求項15に記載の情報処理装置によれば、暗号化手段が、第1の鍵で、第1のデータを第1の暗号に暗号化し、送信手段が、第1の暗号を他の情報処理装置に送信し、受信手段が、他の情報処理装置から、第2の暗号および第3の暗号を受け取り、復号化手段が、第2の暗号を、第2の鍵で第4のデータに復号化するとともに、第3の暗号を、第2の鍵で第5のデータに復号化し、認証手段が、第1のデータと第4のデータに応じて、他の情報処理装置を認証し、暗号化手段が、第

5のデータを、第1の鍵で第4の暗号に暗号化し、送信手段が、第4の暗号を他の情報処理装置に送信するようにしたので、所定の情報処理装置の認証を行うとともに、その情報処理装置により認証されることが可能となる。

【0110】請求項24に記載の情報処理装置によれば、受信手段が、他の情報処理装置により第1の暗号を受け取り、復号化手段が、第1の暗号を、第1の鍵で第1のデータに復号化し、暗号化手段が、第1のデータを、第2の鍵で第2の暗号に暗号化するとともに、第2のデータを、第2の鍵で第3の暗号に暗号化し、送信手段が、第2の暗号および第3の暗号を他の情報処理装置に送信し、受信手段が、他の情報処理装置から第4の暗号を受け取り、復号化手段が、第4の暗号を、第2の鍵で第3のデータに復号化し、認証手段が、第2のデータと第3のデータに応じて、他の情報処理装置を認証するようにしたので、所定の情報処理装置の認証を行うとともに、その情報処理装置により認証されることが可能となる。

#### 【図面の簡単な説明】

【図1】R/W1とICカード2により構成される非接触カードシステムの一例を示す図である。

【図2】本発明の一実施例であるR/W1の構成を示すブロック図である。

【図3】図2の暗号部12の構成例を示すブロック図である。

【図4】図3のデータランダム化部32の構成例を示すブロック図である。

【図5】図2の復号部13の構成例を示すブロック図である。

【図6】本発明の一実施例であるICカード2の構成を

示すブロック図である。

【図7】図1のR/W1の相互認証時の動作について説明するフローチャートである。

【図8】図1のICカード2の相互認証時の動作について説明するフローチャートである。

【図9】図1の非接触カードシステムの相互認証時の動作について説明する図である。

【図10】図1のR/W1の通信時の処理について説明するフローチャートである。

【図11】図1のICカード2の通信時の処理について説明するフローチャートである。

【図12】R/W1とICカード2との通信の他の例を示す図である。

【図13】R/W1とICカード2との通信のさらに他の例を示す図である。

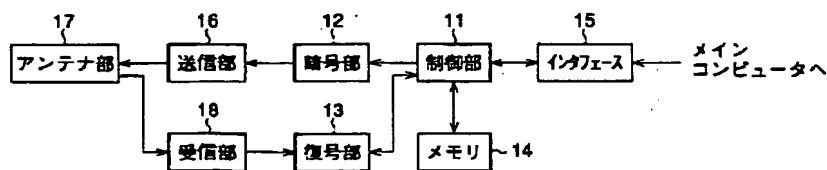
【図14】秘密暗号を利用した通信の一例を示すブロック図である。

【図15】秘密暗号を利用した認証の一例を示すブロック図である。

#### 20 【符号の説明】

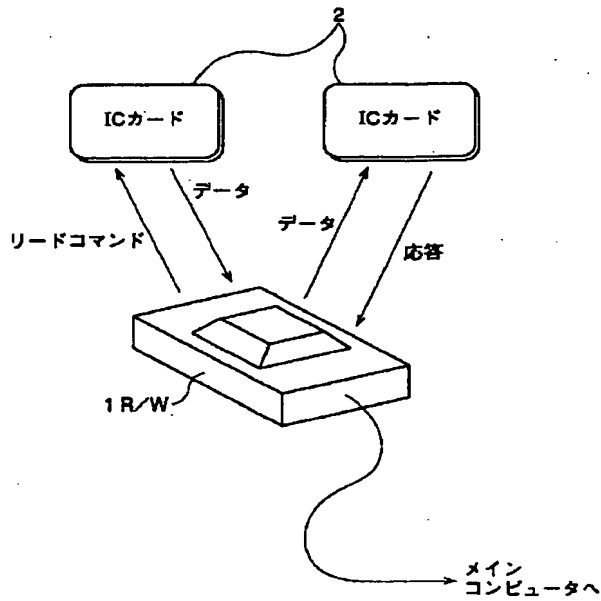
1 リーダ/ライタ (R/W), 2 ICカード,  
11 制御部, 12 暗号部, 13 復号部, 14  
メモリ, 15 インタフェース, 16 送信部,  
17 アンテナ部, 18 受信部, 31 鍵保存部,  
32 データランダム化部, 41 鍵保存部,  
42 変換部, 61 鍵データ生成回路, 62-1  
乃至62-16 演算回路, 63 レジスタ, 64  
-1乃至64-16 加算器, 65 レジスタ, 8  
1 制御部, 82 暗号部, 83 復号部, 84  
メモリ, 86 送信部, 87 アンテナ部, 88  
受信部

【図2】

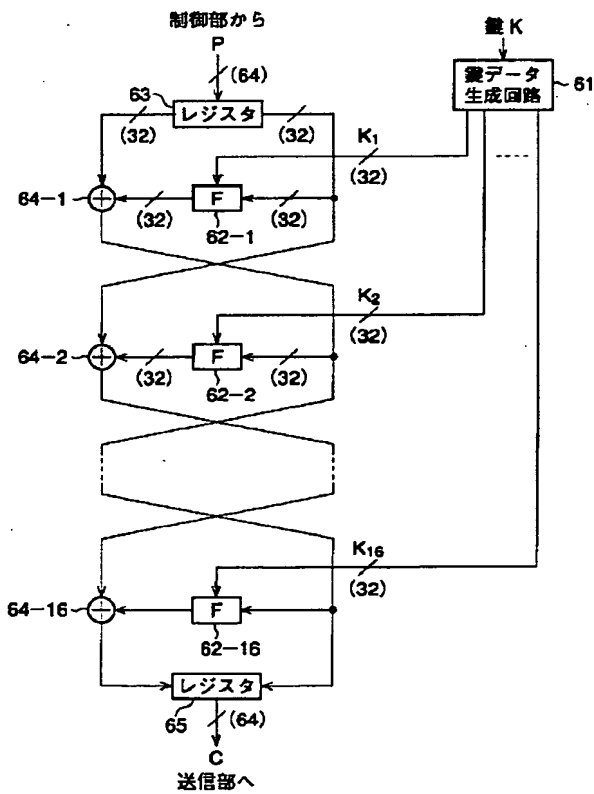


R/W1

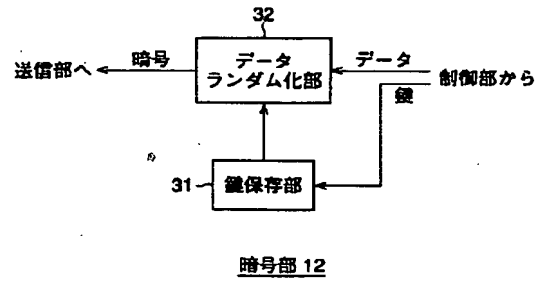
【図1】



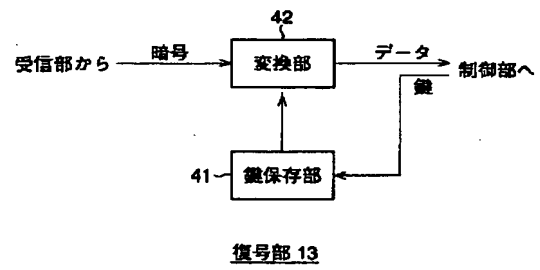
【図4】



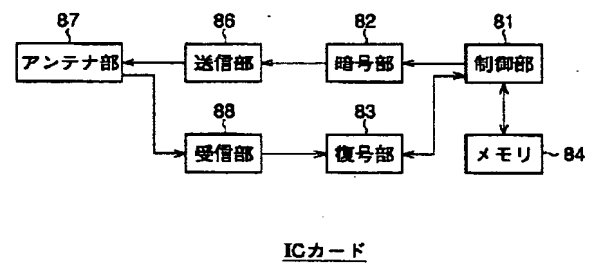
【図3】



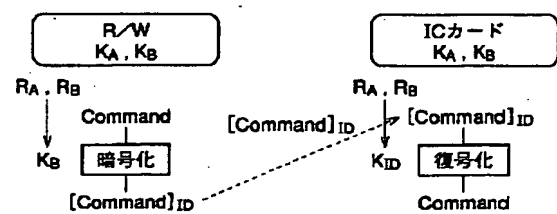
【図5】



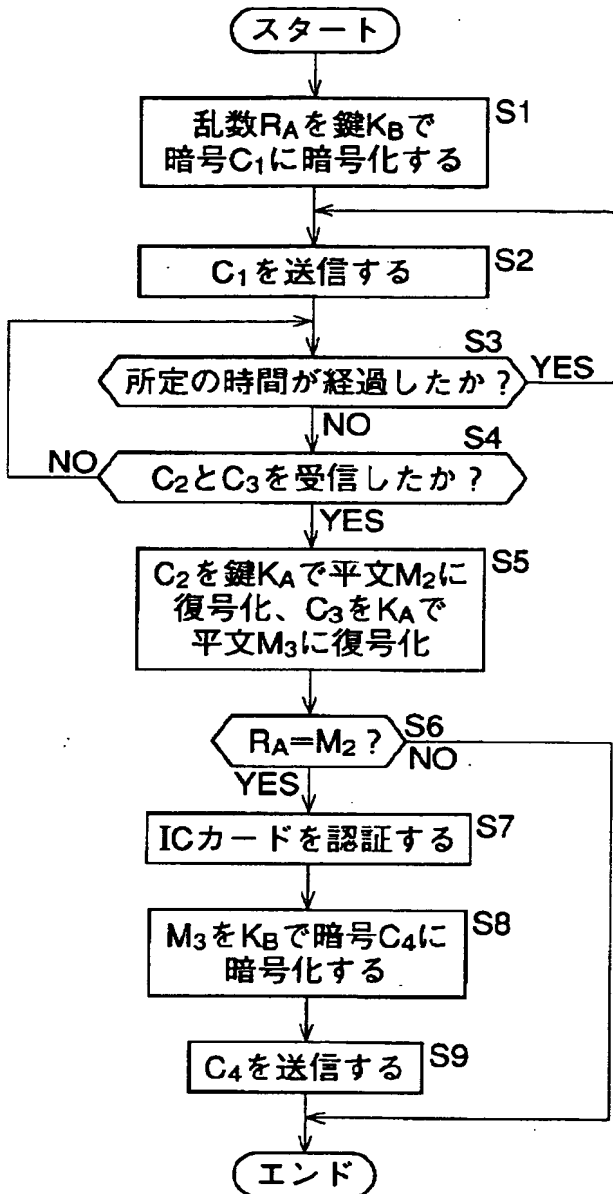
【図6】



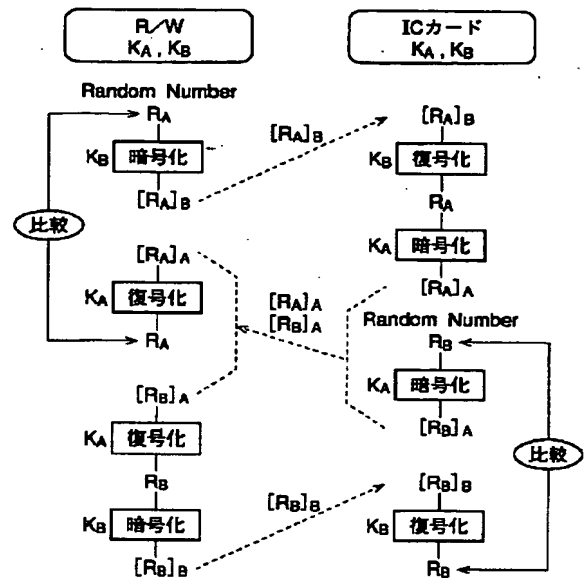
【図12】



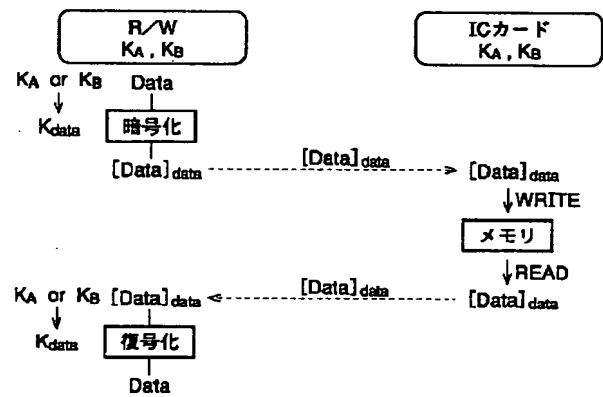
【図7】



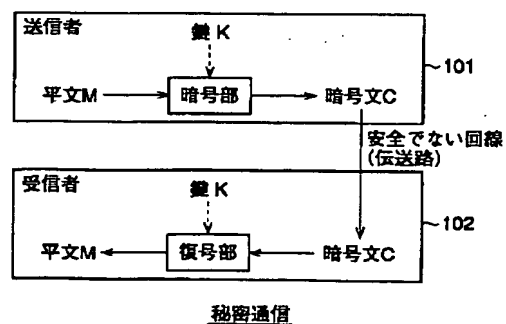
【図9】



【図13】



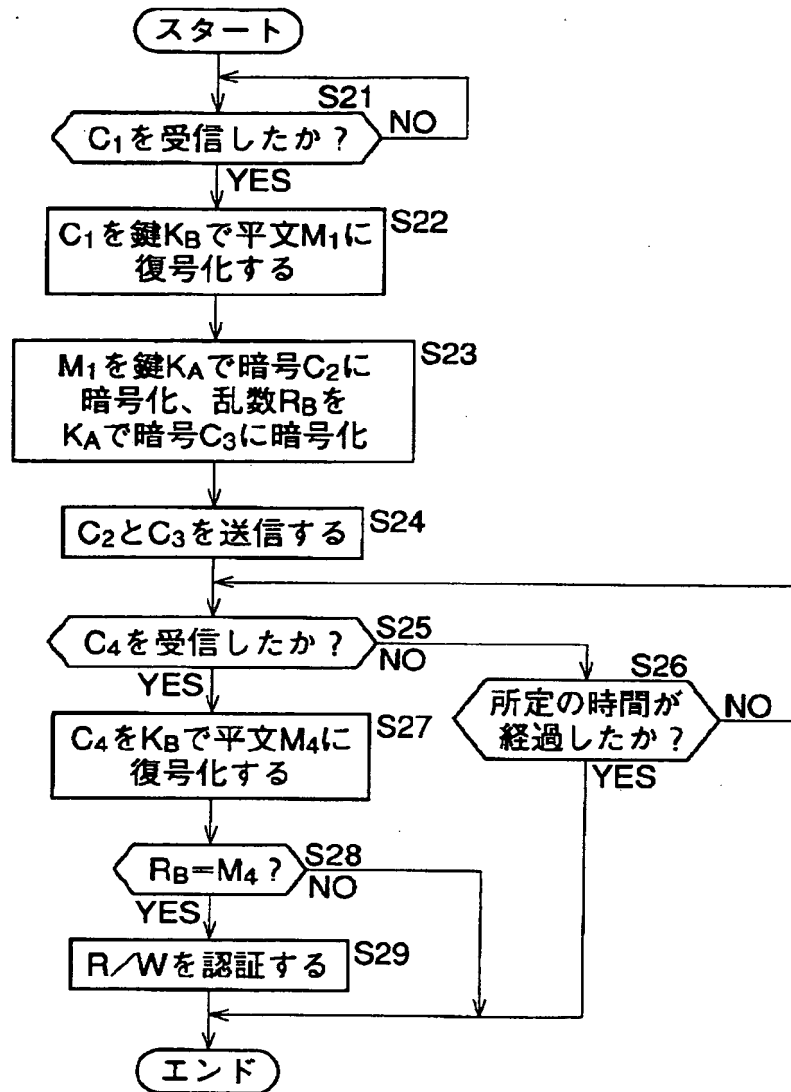
【図14】



R/W1における認証処理

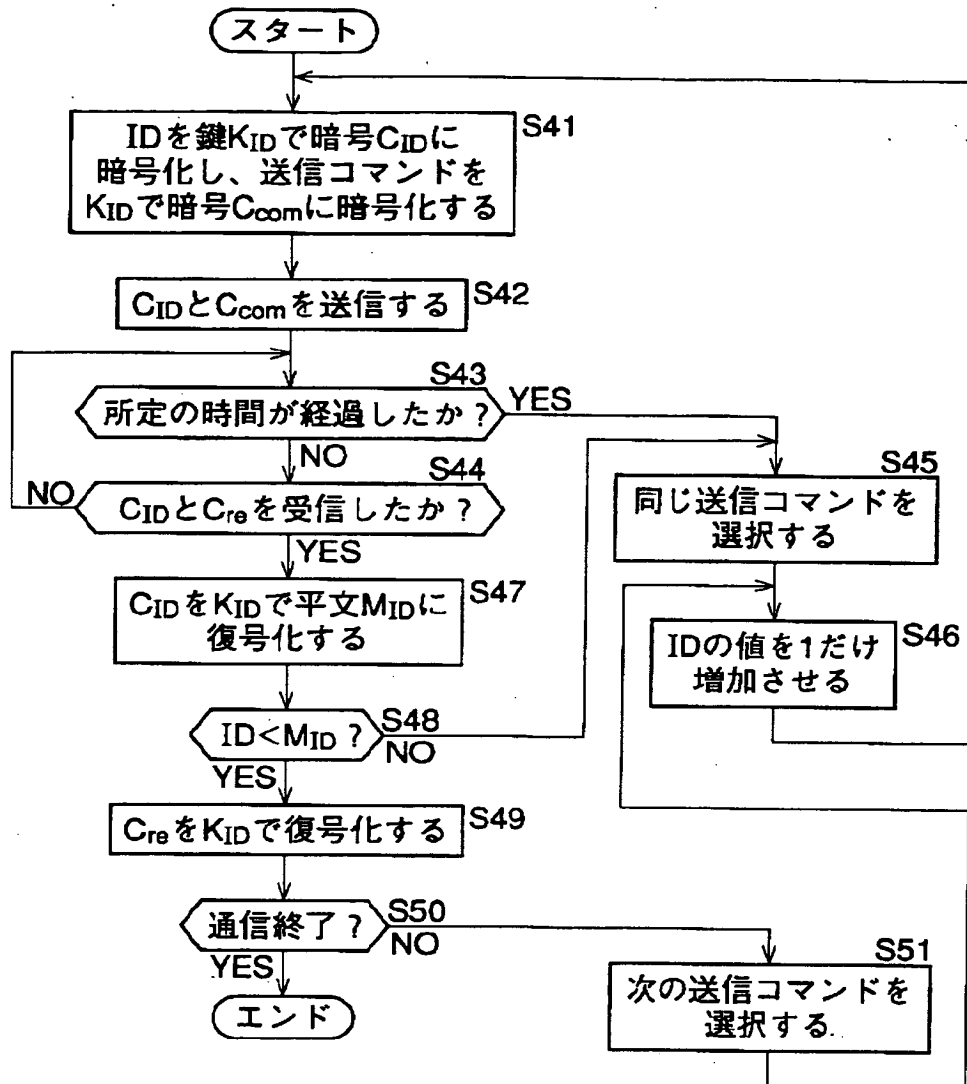


【図8】



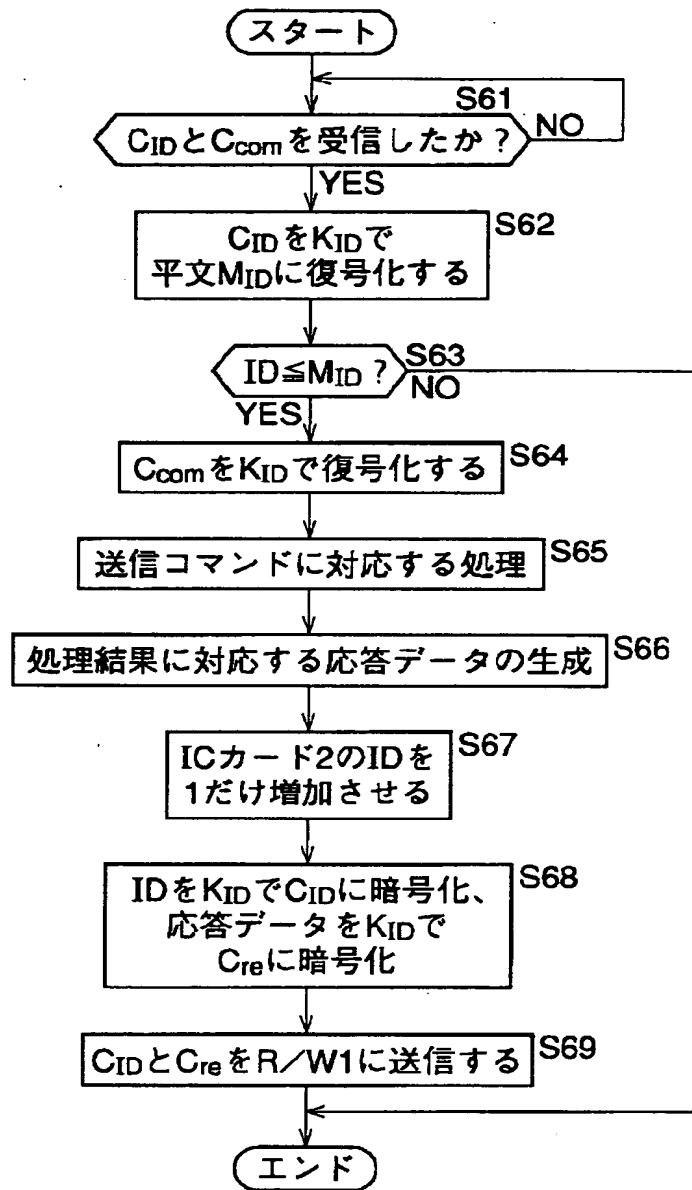
ICカードにおける認証処理

【図10】



R/Wにおける処理

【図11】

ICカードにおける処理

【図15】

